(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
17 janvier 2002 (17.01.2002)

PCT

(10) Numéro de publication internationale
WO 02/05483 A1

(51) Classification internationale des brevets[7] : H04L 9/30

(21) Numéro de la demande internationale :
PCT/FR01/01948

(22) Date de dépôt international : 21 juin 2001 (21.06.2001)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
00 08994 10 juillet 2000 (10.07.2000) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **GEMPLUS** [FR/FR]; Avenue du Pic de Bertagne, Parc d'Activités de GEMENOS, F-13420 GEMENOS (FR).

(72) Inventeurs; et

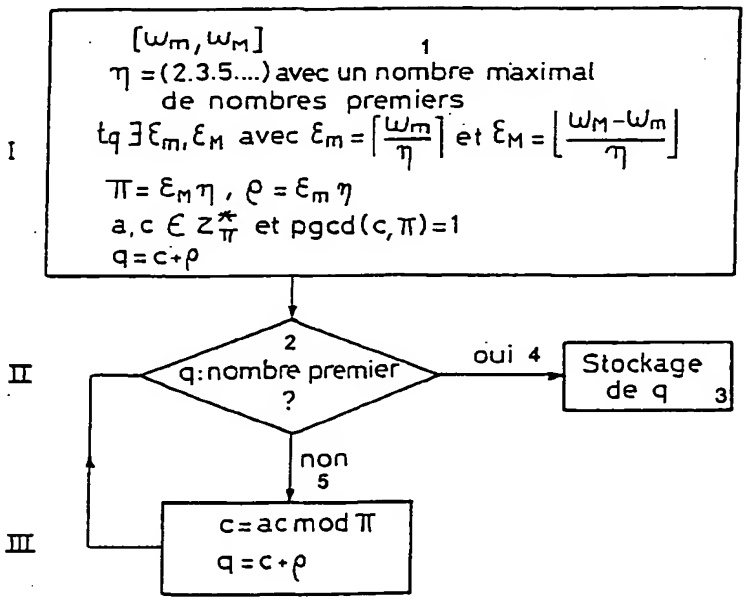
(75) Inventeurs/Déposants *(pour US seulement)* : **JOYE, Marc** [FR/FR]; 19 rue Voltaire, F-83640 SAINT ZACHARIE (FR). **PAILLIER, Pascal** [FR/FR]; 37 Cours de Vincennes, F-75020 PARIS (FR).

(74) Mandataires : **BRUYERE, Pierre** etc.; C/O GEMPLUS, Service brevets, BP 100, F-13881 GEMENOS CEDEX (FR).

[Suite sur la page suivante]

(54) Title: METHOD FOR GENERATING AN ELECTRONIC KEY FROM A PRIME NUMBER CONTAINED IN A SPECIFIC INTERVAL AND DEVICE THEREFOR

(54) Titre : PROCEDE DE GENERATION D'UNE CLE ELECTRONIQUE A PARTIR D'UN NOMBRE PREMIER COMPRIS DANS UN INTERVALLE DETERMINE ET DISPOSITIF DE MISE EN OEUVRE DU PROCEDE



1...WITH A MAXIMUM NUMBER OF PRIME NUMBERS
2...q:PRIME NUMBER ?
3...STORING q
4...YES,
5...NO

(57) **Abstract:** The invention concerns a method for generating an electronic key from a prime number q contained in a specific interval of positive integers (W_m, W_M). Said method comprises the following operations: a) selecting a positive integer η, η being the product of the k first prime numbers, with k as maximum so that there exist two positive integers ε_m and ε_M such that ε_m is the higher roundoff of W_m/η, and ε_M is the lower roundoff of $(W_M - W_m)/\eta$, calculating $\Pi = \varepsilon_M . \eta$ and $\rho = \varepsilon_m . \eta$, generating two positive integers a and c belonging to the multiplicative group Z^*_Π of integers modulo Π, with prime c with Π, calculating $q = c + \rho$; b) testing primality nature of q; c) if primality is verified, q is stored; d) otherwise: updating c by calculating a.c mod Π, repeating the preceding operations as from b) with the new value $q = c + \rho$. The invention is applicable to cryptography.

[Suite sur la page suivante]

WO 02/05483 A1

(81) **États désignés** *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) **États désignés** *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— *avec rapport de recherche internationale*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

(57) Abrégé : L'invention concerne un procédé de génération d'une clé électronique à partir d'un nombre premier q compris dans un intervalle de nombres entiers positifs déterminé $[W_m, W_M]$. Ce procédé comprend les opérations suivantes: a) choix d'un nombre entier positif η, η étant le produit des k premiers nombres premiers, avec k maximum pour qu'il existe deux nombres entiers positifs ε_m et ε_M tels que ε_m est l'arrondi supérieur de w_m/η, et e_M est l'arrondi inférieur de $(W_M-W_m)/\eta$, calcul de $\Pi = \varepsilon_M.\eta$ et $\rho = \varepsilon_m.\eta$, génération de deux nombres entiers positifs a et c appartenant au groupe multiplicatif $Z^*\Pi$ des nombres entiers modulo Π, avec c premier avec Π calcul de $q = c + \rho$ b) test de la primalité de q, c) dans le cas où la primalité est vérifiée, on mémorise q, d) dans le cas contraire: on met à jour c en calculant a.c mod Π, on réitère les opérations précédentes à partir de b) avec la nouvelle valeur $q = c+\rho$. L'invention s'applique à la cryptographie.

PROCEDE DE GENERATION D'UNE CLE ELECTRONIQUE A PARTIR D'UN NOMBRE PREMIER COMPRIS DANS UN INTERVALLE DETERMINE ET DISPOSITIF DE MISE EN OEUVRE DU PROCEDE

L'invention concerne un procédé de génération d'une clé électronique à partir d'un nombre premier q compris dans un intervalle de nombres entiers positifs déterminé $[w_m, w_M]$. L'invention concerne également un dispositif de mise en œuvre du procédé.

L'invention s'applique tout particulièrement à des protocoles de cryptographie à clé publique utilisés pour le cryptage d'informations et/ou l'authentification entre deux entités et/ou la signature électronique de messages.

Elle s'applique en particulier à des protocoles de cryptographie à clé publique tels que le protocole RSA (Rivest Shamir et Adelman), El Gamal, Schnorr, ou Fiat Shamir.

Dans le cas de telles applications, on fait appel à la génération de grands nombres premiers (pouvant être par exemple supérieurs ou égaux à 512 bits) pour former une ou plusieurs clés du protocole.

Une première méthode dite "naïve" de génération de nombre premier consiste à :

- choisir un candidat parmi les nombres impairs,
- tester sa primalité,
- si la primalité est vérifiée, on mémorise ce nombre, sinon, on met à jour le candidat en l'incrémentant de 2, on réitère le test avec ce nouveau candidat et ainsi de suite jusqu'à ce que la primalité d'un candidat soit vérifiée.

Cette méthode est très lente. Une autre méthode consiste à choisir les candidats au test de primalité parmi les nombres premiers avec un nombre premier Π. On rappelle que deux nombres sont premiers entre eux ou co-premiers si et seulement si leur plus grand commun diviseur (pgcd) est égal à 1. Cette autre méthode consiste à :

- considérer le nombre Π = 2.3.5.7.... qui est le produit des k premiers nombres premiers (souvent k = 4) et à choisir un nombre p tel que p soit premier avec Π,
- tester la primalité de p,
- si la primalité de p est vérifiée, on mémorise ce nombre, sinon on met à jour p en l'incrémentant de Π. Ce nouveau candidat p est également premier avec Π ; en effet, on rappelle que

$$pgcd(p+\Pi, \Pi) = pgcd(p, \Pi) = 1$$

- on réitère le test avec ce nouveau candidat et ainsi de suite jusqu'à ce que l'on ait trouvé un candidat qui soit un nombre premier.

Cette méthode est plus efficace.

Mais on souhaite en général générer un nombre premier dans un intervalle déterminé. En effet, dans le cas par exemple du protocole de cryptographie à clé publique RSA, on considère le produit de 1024 bits de deux nombres premiers p et q, c'est-à-dire $2^{511}.\sqrt{2}<p,q<2^{512}$. Selon un autre protocole basé sur le logarithme discret, on cherche directement à obtenir un nombre premier de 1024 bits, c'est-à-dire $2^{1023}<p<=2^{1024}$. Ces protocoles s'avèrent difficiles à programmer sur des dispositifs portables de type carte à

microprocesseur (car complexes) et de performances médiocres pour des nombres de grandes tailles usuelles, 512 bits, 1024 bits voire plus.

L'invention a pour but, étant donné l'intervalle $[w_m, w_M]$, de déterminer Π une fois pour toutes et de proposer une mise à jour du candidat garantissant que le nouveau candidat sera premier avec Π dans l'intervalle déterminé initialement tout en maintenant le temps de calcul de ces nouveaux candidats dans des limites raisonnables, c'est-à-dire en limitant le nombre de tests de primalité.

Le choix de Π est illustré par la figure 1 où sont représentés l'ensemble I des entiers compris dans un intervalle $[w_m, w_M]$, dans lequel est inclus l'ensemble $I\Pi$ des entiers de cet intervalle premiers avec Π, dans lequel est inclus l'ensemble IP des nombres premiers de cet intervalle. Le but consiste à déterminer Π de façon à ce que l'ensemble intermédiaire $I\Pi$ des entiers premiers avec Π, c'est-à-dire l'ensemble des candidats, soit le plus proche possible du sous-ensemble IP des nombres premiers de l'intervalle.

L'invention a plus particulièrement pour objet un procédé de génération d'une clé électronique à partir d'un nombre premier q compris dans un intervalle de nombres entiers positifs déterminé $[w_m, w_M]$, principalement caractérisé en ce que le nombre premier q est obtenu en réalisant les opérations suivantes :

a) choix d'un nombre entier positif η, η étant le produit des k premiers nombres premiers, avec k maximum pour qu'il existe deux nombres entiers positifs ε_m et ε_M tels que ε_m est l'arrondi supérieur de w_m/η, et ε_M est l'arrondi inférieur de $(w_M-w_m)/\eta$,

calcul de $\Pi = \varepsilon_M.\eta$ et $\rho = \varepsilon_m.\eta$,

génération de deux nombres entiers positifs a et c appartenant au groupe multiplicatif Z^*_Π des nombres entiers modulo Π, avec c premier avec Π

calcul de $q = c + \rho$

b) test de la primalité de q,

c) dans le cas où la primalité est vérifiée, on mémorise q,

d) dans le cas contraire :

on met à jour c en calculant a.c mod Π,

on réitère les opérations précédentes à partir de b) avec la nouvelle valeur $q = c+\rho$.

Selon une caractéristique de l'invention, $a = 2$ et $\Pi = (\varepsilon_M-1).\eta$.

Selon une autre caractéristique, $a = 2^{16} + 1$.

L'invention s'applique aux procédés de génération de clés cryptographiques RSA, El Gamal, Schnorr, ou Fiat Shamir.

L'invention a également pour objet un dispositif électronique portable comprenant un processeur

arithmétique et une mémoire de programme associée, apte à effectuer des calculs modulaires, principalement caractérisé en ce qu'il comprend un programme de vérification de primalité d'un nombre entier positif q compris dans un intervalle de nombres entiers positifs déterminé $[w_m, w_M]$ qui effectue les opérations suivantes :

a) choix d'un nombre entier positif η, η étant le produit des k premiers nombres premiers, avec k maximum pour qu'il existe deux nombres entiers positifs ε_m et ε_M tels que ε_m est l'arrondi supérieur de w_m/η, et ε_M est l'arrondi inférieur de $(w_M-w_m)/\eta$,

calcul de $\Pi = \varepsilon_M.\eta$ et $\rho = \varepsilon_m.\eta$,

génération de deux nombres entiers positifs a et c appartenant au groupe multiplicatif Z^*_Π des nombres entiers modulo Π, avec c premier avec Π

calcul de $q = c + \rho$

b) test de la primalité de q,

c) dans le cas où la primalité est vérifiée, le processeur arithmétique stocke q,

d) dans le cas contraire :

mise à jour de c par le calcul de a.c mod Π,

le processeur arithmétique réitère les opérations précédentes à partir de b) avec $q = c+\rho$.

Avantageusement, le dispositif électronique portable est constitué par une carte à puce à microprocesseur.

D'autres particularités et avantages de l'invention apparaîtront clairement à la lecture de la description faite à titre d'exemple non limitatif et en regard des dessins annexés sur lesquels :

la figure 1 représente l'ensemble I des entiers compris dans un intervalle $[w_m, w_M]$, l'ensemble III des entiers de cet intervalle premiers entre eux et enfin l'ensemble IP des nombres premiers de cet intervalle,

la figure 2 représente l'organigramme du procédé selon l'invention,

la figure 3 représente le schéma de principe d'un dispositif électronique portable tel qu'une carte à puce mettant en œuvre le procédé selon l'invention.

Le but de l'invention consiste donc dans un premier temps à déterminer Π de façon à ce que l'ensemble III des entiers premiers avec Π représenté figure 1 soit le plus proche possible du sous-ensemble IP des nombres premiers de l'intervalle.

Selon l'invention, le procédé représenté figure 2 est initialisé de la manière suivante (étape I):

pour générer un nombre premier q tel que $q \in [w_m, w_M]$,

on choisit un nombre η de la même forme que Π (η est le produit des k' premiers nombres premiers) où k' est maximum et tel qu'il existe deux nombres entiers

positifs ε_m et ε_M tels que ε_m est l'arrondi supérieur de w_m/η, que l'on note $\lceil w_m/\eta \rceil$ et ε_M est l'arrondi inférieur de $(w_M-w_m)/\eta$ que l'on note $\lfloor (w_M-w_m)/\eta \rfloor$.

Π est alors obtenu en posant $\Pi = \varepsilon_M.\eta$; on pose également $\rho = \varepsilon_m.\eta$

On remarque que Π est proche de w_M-w_m mais inférieur et que ρ est proche de w_m mais supérieur.

Il faut à présent déterminer la mise à jour des candidats de façon à ce que les nouveaux candidats appartiennent toujours à $I\Pi$.

On considère l'anneau Z_Π des entiers modulo Π et Z^*_Π le groupe multiplicatif de Z_Π ; on remarque que l'ensemble $(\rho + Z^*_\Pi)$ est inclus dans et quasiment identique à $I\Pi$, c'est-à-dire à l'ensemble des candidats.

On génère alors deux nombres entiers positifs a et c appartenant à ce groupe multiplicatif Z^*_Π avec c premier avec Π (c'est-à-dire $pgcd(c, \Pi)=1$) et on considère le candidat $q = c + \rho$ (étape I). Pour générer c, on utilise un algorithme de génération de nombres co-premiers tel qu'il en existe dans la littérature.

Comme ρ est proche de w_m et que $c<\Pi$, on vérifie automatiquement que $w_m<q<w_M$.

Par ailleurs, $pgcd(q,\Pi)= pgcd(c+\rho,\Pi)= pgcd(c, \Pi)=1$
On vérifie ainsi que q appartient effectivement à $I\Pi$.

Cette phase d'initialisation terminée, on teste la primalité du candidat q (étape II). Si elle est vérifiée, on mémorise q, sinon :

on met à jour c en calculant a.c mod Π et on calcule le nouveau candidat $q = c + \rho$ (étape III).

Le nouveau candidat appartient à l'ensemble $I\Pi$: en effet, en raison des propriétés des groupes multiplicatifs, a et c appartenant à Z^*_Π, le produit a.c appartient aussi à ce groupe Z^*_Π ainsi que a.c mod Π.

Les protocoles de cryptographie à clé publique sont souvent mis en œuvre sur des cartes à puce à microprocesseur. Par exemple, dans le protocole RSA, les clés sont générées à partir de nombres choisis de manière aléatoire par la carte à microprocesseur à l'exécution du protocole. A cette fin, la carte à microprocesseur possède un générateur de nombres aléatoires, capable de fournir un nombre entier de la taille désirée.

On a donc représenté sur la figure 3 le schéma fonctionnel d'une carte à microprocesseur susceptible de mettre en œuvre le procédé selon l'invention.

La carte C comporte une unité principale de traitement 1, des mémoires de programmes 3 et 4 et une mémoire de travail (non représentée), associées à l'unité 1. La carte comporte également un processeur arithmétique 2 capable d'effectuer des calculs modulaires et une mémoire sécurisée 6 (non accessible de l'extérieur) dans laquelle sera stockée le candidat q dont la primalité aura été vérifiée. La carte possède

également un générateur de nombres entiers aléatoires 5.

En vue de la mise en œuvre du procédé en particulier sur une carte à microprocesseur telle que décrite, il est souhaitable d'augmenter la vitesse du traitement mis en œuvre par le procédé (opérations effectuées par le processeur arithmétique 2) et de libérer de l'emplacement dans la mémoire de travail.

Dans ce but, en choisissant a = 2 et en excluant 2 du nombre Π (Π = 3.5.7. ...), on évite les calculs modulaires. En effet, la mise à jour de c devient 2c mod Π. Or comme c est un élément de Z^*_Π, 2c mod Π = 2c ou 2c - Π.

Mais, les nouveaux candidats q peuvent alors être pairs. Si c'est le cas, on ajoute alors au nouveau candidat un nombre tel que le nouveau candidat devienne impair tout en appartenant toujours à l'ensemble III. On pose ainsi :

$\Pi = (\varepsilon_M - 1).\eta$

$q = c + \rho$

si q est pair alors q devient $q + \eta$.

Selon une autre alternative, on peut garder Π tel que défini initialement et choisir une valeur particulière de a telle que a soit premier avec Π. On peut choisir par exemple $a = 2^{16} + 1$.

Le procédé selon l'invention a été mis en œuvre sur une plate-forme de carte à puce SLE66CX160S d'Infineon

comprenant une unité centrale 8-bit et un crypto-processeur arithmétique 1100-bit. En choisissant pour η, Π et ρ les valeurs suivantes :

η=b16bd1e084af628fe5089e6dabd16b5b80f60681d6a092fcb
1e86d82876ed71921000bcfdd063fb90f81dfd07a021af23c735d52
e63bd1cb59c93cbb398afd$_{16}$,

$\Pi = 1729.\eta$

$\rho = 4180.\eta$,

on obtient avec a = 2, un nombre premier de 512 bits en moins de 4 secondes. On obtient par conséquent un nombre premier de 1024 bits en moyenne en moins de 8 secondes.

REVENDICATIONS

1. Procédé de génération d'une clé électronique à partir d'un nombre premier q compris dans un intervalle de nombres entiers positifs déterminé $[w_m, w_M]$, caractérisé en ce que le nombre premier q est obtenu en réalisant les opérations suivantes :

a) choix d'un nombre entier positif η, η étant le produit des k premiers nombres premiers, avec k maximum pour qu'il existe deux nombres entiers positifs ε_m et ε_M tels que ε_m est l'arrondi supérieur de w_m/η, et ε_M est l'arrondi inférieur de $(w_M-w_m)/\eta$,

calcul de $\Pi = \varepsilon_M.\eta$ et $\rho = \varepsilon_m.\eta$,

génération de deux nombres entiers positifs a et c appartenant au groupe multiplicatif Z^*_Π des nombres entiers modulo Π, avec c premier avec Π

calcul de $q = c + \rho$

b) test de la primalité de q,

c) dans le cas où la primalité est vérifiée, on mémorise q,

d) dans le cas contraire :

on met à jour c en calculant $a.c \bmod \Pi$,

on réitère les opérations précédentes à partir de b) avec la nouvelle valeur $q = c+\rho$.

2. Procédé selon la revendication précédente, caractérisé en ce que $a = 2$ et $\Pi = (\varepsilon_M - 1).\eta$.

3. Procédé selon la revendication 1, caractérisé en ce que $a = 2^{16} + 1$.

4. Procédé de génération de clés cryptographiques RSA, El Gamal, Schnorr, ou Fiat Shamir, caractérisé en ce qu'il met en œuvre le procédé selon l'une quelconque des revendications précédentes.

5. Dispositif électronique portable comprenant un processeur arithmétique et une mémoire de programme associée, apte à effectuer des calculs modulaires, caractérisé en ce qu'il comprend un programme de vérification de primalité d'un nombre entier positif q compris dans un intervalle de nombres entiers positifs déterminé $[w_m, w_M]$ et qui effectue les opérations suivantes :

a) choix d'un nombre entier positif η, η étant le produit des k premiers nombres premiers, avec k maximum pour qu'il existe deux nombres entiers positifs ε_m et ε_M tels que ε_m est l'arrondi supérieur de w_m/η, et ε_M est l'arrondi inférieur de $(w_M - w_m)/\eta$,

calcul de $\Pi = \varepsilon_M.\eta$ et $\rho = \varepsilon_m.\eta$,

génération de deux nombres entiers positifs a et c appartenant au groupe multiplicatif Z^*_Π des nombres entiers modulo Π, avec c premier avec Π

calcul de $q = c + \rho$

b) test de la primalité de q,

c) dans le cas où la primalité est vérifiée, le processeur arithmétique stocke q,

d) dans le cas contraire :

mise à jour de c par le calcul de a.c mod Π,

le processeur arithmétique réitère les opérations précédentes à partir de b) avec $q = c+\rho$.

6. Dispositif électronique portable selon la revendication 5, caractérisé en ce qu'il est constitué par une carte à puce à microprocesseur.

FIG_1

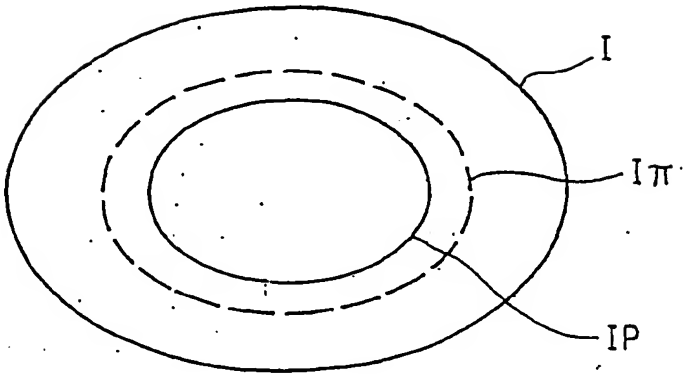

I
Iπ
IP

FIG_2

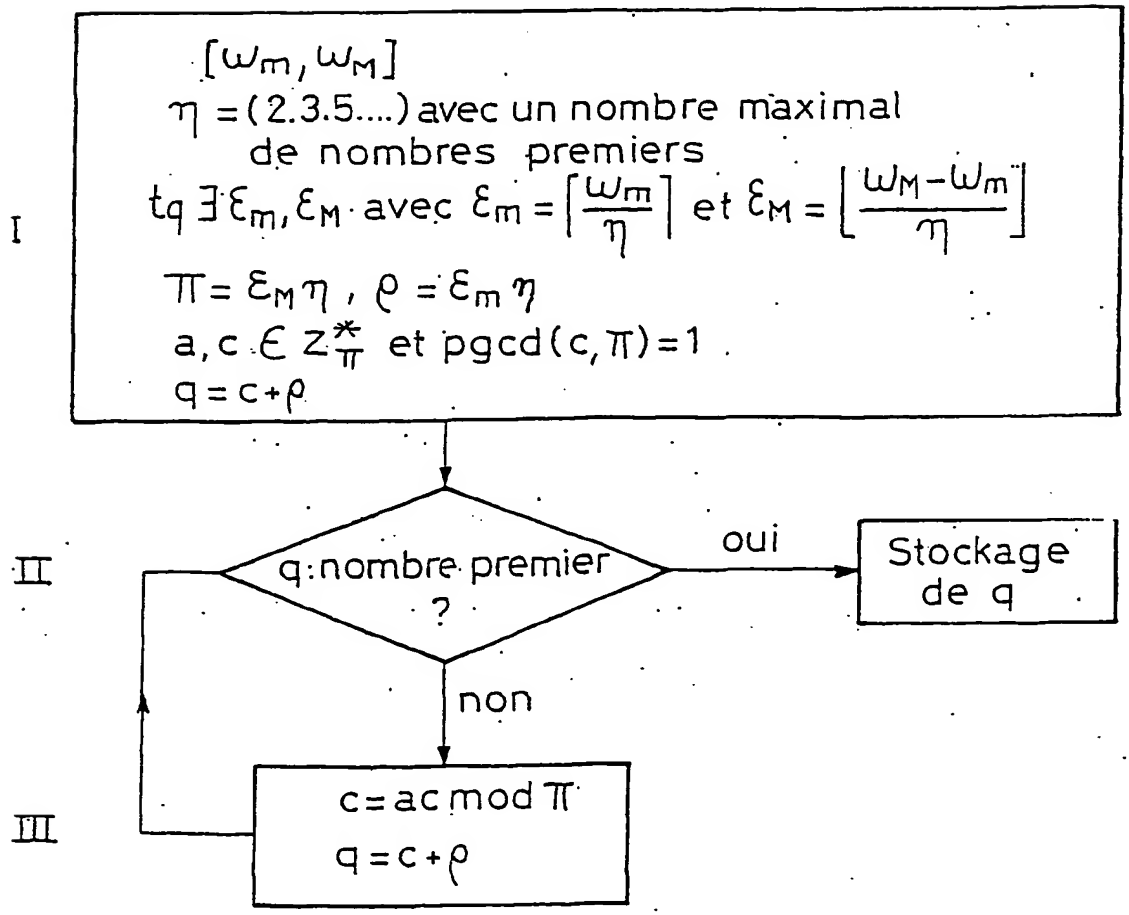
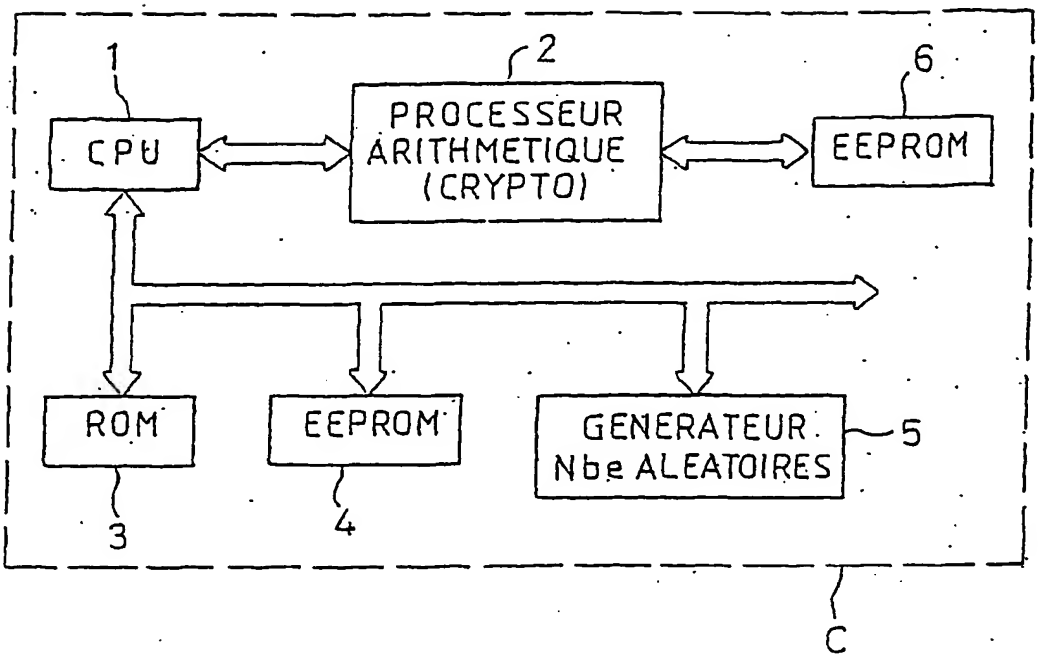

I
$[\omega_m, \omega_M]$
$\eta = (2.3.5....)$ avec un nombre maximal de nombres premiers
tq $\exists \varepsilon_m, \varepsilon_M$ avec $\varepsilon_m = \left\lceil \frac{\omega_m}{\eta} \right\rceil$ et $\varepsilon_M = \left\lfloor \frac{\omega_M - \omega_m}{\eta} \right\rfloor$
$\pi = \varepsilon_M \eta$, $\rho = \varepsilon_m \eta$
$a, c \in Z_\pi^*$ et $pgcd(c, \pi) = 1$
$q = c + \rho$
II
q: nombre premier ?
oui
Stockage de q
non
III
$c = ac \bmod \pi$
$q = c + \rho$

FIG_3


1
2
6
CPU
PROCESSEUR ARITHMETIQUE (CRYPTO)
EEPROM
ROM
EEPROM
GENERATEUR Nbe ALEATOIRES
5
3
4
C

INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 01/01948

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, INSPEC, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	YASUKO GOTOH ET AL: "A METHOD FOR RAPID RSA KEY GENERATION" SYSTEMS & COMPUTERS IN JAPAN,SCRIPTA TECHNICA JOURNALS. NEW YORK,US, vol. 21, no. 8, 1990, pages 11-20, XP000177817 ISSN: 0882-1666 page 13, right-hand column, line 8 -page 14, right-hand column, line 5	1

☐ Further documents are listed in the continuation of box C.

☐ Patent family members are listed in annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 October 2001	22/10/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
PCT/FR 01/01948

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 H04L9/30

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, INSPEC, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
A	YASUKO GOTOH ET AL: "A METHOD FOR RAPID RSA KEY GENERATION" SYSTEMS & COMPUTERS IN JAPAN,SCRIPTA TECHNICA JOURNALS. NEW YORK,US, vol. 21, no. 8, 1990, pages 11-20, XP000177817 ISSN: 0882-1666 page 13, colonne de droite, ligne 8 -page 14, colonne de droite, ligne 5	1

☐ Voir la suite du cadre C pour la fin de la liste des documents

☐ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
12 octobre 2001	22/10/2001

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G